УДК 004.056
Р. Яворський, В. Амбок, В. Леньо
Тернопільський національний технічний університет імені Івана Пулюя

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РОЗГОРТАННІ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

UDC 004.056
R. Yavorskii, V. Ambok, V. Lenio
(Ternopil Ivan Puluj National Technical University, Ukraine)

INFORMATION SECURITY CHALANGES FOR DEPLOYMENT OF INTRUSION DETECTION SYSTEMS

Розглянемо основні класи небезпек, характерних для розгортання систем виявлення вторгнень на основі віртуальних машин – Virtual Machines (VM), оскільки саме вони є основним елементом побудови інформаційної інфраструктури організації у хмарних сервісах [1].

VM image sharing. Вважається, що існує репозиторій образів різних VM, а користувач на їх основі може сконфігурувати потрібний образ. Таке використання образів з репозиторію може спричинити появу вразливостей у системі [2]. Зловмисник може знайти вразливості в існуючому образі або завантажити у репозиторій власний, шкідливий, образ VM.

VM isolation. З іншого боку проблему становить використання VM в ізоляції від інших віртуальних машин, що працюють на тому ж комп'ютері. Очевидно, що вони мають бути ізольовані одна від одної. Попри логічну ізоляцію існує проблема доступу до спільних ресурсів (пам'яті, дискового простору). Через що виникає проблема крос-VM атак.

VM escape. Це ситуація, коли зловмисник обходить систему управління VM [3]. В цьому випадку зловмисник отримає доступ до інших VM, що може спричинити також неавторизований доступ до файлів на жорстких дисках. До таких вразливостей в основному схильні системи
IaaS [4].

VM migration. Під час міграції весь інформаційний контент VM стає відкритим при передачі даних по мережі [5]. На додачу модуль міграції може бути скомпрометований атакуючим зловмисником для переміщення VM на сторонній сервер. Тому критично важливим є виконання операції міграції VM з дотриманням всіх заходів безпеки.

Безпечне управління образами забезпечується за допомогою спеціально розробленого фреймворку, згідно якого кожну операцію може виконувати тільки авторизований користувач. Крім того рекомендується використовувати журналювання всіх операцій.

Література

1. F. Sabahi, “Secure Virtualization for Cloud Environment Using Hypervisor-based Technology,” Int. Journal of Machine Learning and Computing, vol. 2, no. 1, 2012.
2. S.-F. Yang, W.-Y. Chen, and Y.-T. Wang, “ICAS: An inter-VM IDS Log Cloud Analysis System,” in 2011IEEE International Conference on Cloud Computing and Intelligence Systems, 2011, pp. 285–289.
3. S. L. and Z. L. and X. C. and Z. Y. and J. Chen, S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, “Virtualization security for cloud computing service,” in International Conference on Cloud and Service Computing (CSC), 2011, pp. 174–179.
4. M. Ibrahim, A.S. and Hamlyn-Harris, J. and Grundy, J. and Almorsy, “CloudSec: A security monitoring appliance for Virtual Machines in the IaaS cloud model,” in 5th International Conference on Network and System Security (NSS), 2011, pp. 113–120.
5. J. Sedayao, S. Su, X. Ma, M. Jiang, and K. Miao, “A Simple Technique for Securing Data at Rest Stored in a Computing Cloud,” in Proceedings of the 1st International Conference on Cloud Computing, 2009, pp. 553–558.